Impact of Security Management Activities on Corporate Performance

Hyunwoo Cho and Keuntae Cho *

Posted Date: 19 June 2025

doi: 10.20944/preprints202506.1578.v1

Keywords: security management activities; corporate performance; multiple regression analysis; moderating effect analysis; ISMS (information security management system); IT investment proportion

Article

Impact of Security Management Activities on Corporate Performance

Hyunwoo Cho [1], Keuntae Cho [2,*]

[1] Graduate School of Management of Technology, Sungkyunkwan University, Suwon 16419, Republic of Korea

[2] Department of Systems Management Engineering, Sungkyunkwan University, 2066 Seobu-ro, Jangan-gu, Suwon 16419, Republic of Korea

* Correspondence: ktcho@skku.edu; Tel.: +82_031_290_7602

Abstract: The digital business environment is evolving rapidly due to the development of new information technology (IT). Consequently, information security incidents in organizations have reached a situation that threatens management. This study examines whether managers' security management activities can serve as active innovation factors. Specifically, it analyzes their link to corporate performance, including sales, rather than viewing them merely as defensive risk management. To this end, multiple regression and moderation effect analyses were conducted. These analyses used the IS disclosure data from 545 companies reported to government agencies, along with the financial data of the sample companies. The results indicate a significant negative effect of the IT investment proportion on sales. However, possessing security management tools such as an information security management system (ISMS) positively moderates this relationship. This study provides practical guidance for managers who wish to incorporate security management activities as innovation factors in their management strategies.

Keywords: security management activities; corporate performance; multiple regression analysis; moderating effect analysis; ISMS (information security management system); IT investment proportion

1. Introduction

In 2024, an information security incident occurred that was considered the worst telecommunications hack in US history. The hacker group "Salt Typhoon," believed to be linked to the Chinese government, breached several US telecommunications companies, including AT&T, Verizon, and T-Mobile. The hack included communications from the presidential campaign teams of Donald Trump and Kamala Harris, which ultimately became a national issue.

The private sector was no exception. In February 2024, Change Healthcare, a medical billing and insurance processing company, suffered a ransomware attack by the Russian hacker group ALPHV/BlackCat. This incident resulted in the leak of patient data for more than 100 million people. The leaked information included not only patient contact information but also financial and health information, forcing the company to pay a ransom of $22 million [2]. These security incidents have caused severe economic losses and significant national and societal reper-cussions. Consequently, security management strategies have become essential components of national institutions and corporate strategies [3]. Moreover, they are increasingly seen as sources of external competitiveness for organizations [4].

This study aims to integrate diverse academic and practical insights. It considers corporate security management activities as innovative elements of technology management and also offers recommendations for public institutions and corporations from a managerial perspective [6]. Additionally, it seeks to objectively verify the role of security management activities using real-world

 doi:10.20944/preprints202506.1578.v1

data. Specifically, this study examines whether these activities serve merely as passive risk management measures or as proactive strategic elements. It also explores their direct impact on corporate performance metrics, such as actual sales revenue [7].

With the efforts of international organizations and governments, the information security management system (ISMS) has become a widely adopted information security management tool. Government authorities actively recommend its implementation in most public institutions and corporations. This study also examines the role of ISMS in the relationship between security management activities and corporate performance [8,9].

Previous studies on information security have primarily focused on the inherent objectives of information protection. This focus has resulted in a limited measurement of direct correlations with corporate performance. Consequently, intuitive explanatory power regarding corporate outcomes has been insufficient [10]. However, this study accepts prior research suggesting that information security as a form of institutional regulation and managerial constraint can lead to innovative activities essential for corporate survival [11,12]. This study empirically verifies whether corporate security management activities serve as innovative managerial elements.

We utilized information security disclosure data from 545 sample companies available on a government portal, along with financial data collected by financial institutions. The sample includes companies with assets of over 300 billion won, categorized by industrial classification codes reported to the National Statistical Office.

Chapter 2 systematically reviews the literature on security management activities. Chapter 3 describes the research methods, including data collection and analysis techniques. Chapter 4 presents the research results, verifying the multiple regression analysis of independent variables with the simultaneous input of control variables. It also examines the interaction effects of the moderator variables for each independent variable. Chapter 5 discusses the research findings based on the interpretation of the results, and Chapter 6 summarizes the significance and limitations, offering implications for future research.

2. Literature Review and Hypothesis Setting

2.1. Security Management Activities

Information security refers to measures that protect an organization's important structured or unstructured information from unauthorized access, leakage, use, or alteration. Although the official term used in the current national legal framework is "information protection," businesses commonly use various terms such as "information security" or "IT security" [5].

In this study, we use the terms "information security" and "security management activities" from a management perspective. In other words, it involves developing and delivering products and services essential to business management through an understanding of IT. Simultaneously, this approach proactively prevents hidden security vulnerabilities and improves operational efficiency. Ultimately, it can be defined as part of a management strategy to gain a competitive advantage in the market. Recent cases of Chinese companies growing rapidly due to the leakage of important technical information from South Korea and Japan have been reported. These cases have highlighted the importance of security management activities [5].

Companies must implement security management strategies. Certain management resources must be invested to achieve efficient information security goals that align with management objectives [5,10,37]. This study defines information security activities that do not involve financial costs as non-financial security management activities. Financial security management activities involve financial costs.

2.2. Non-Financial Security Management Activities

2.2.1. Internal Security Management Activities and Corporate Performance

 doi:10.20944/preprints202506.1578.v1

Managers carry out several security management activities internally, either due to legal obligation or corporate initiative, to ensure information security.

First, annual information security education is mandated for all organization members under Article 28 of the Personal Information Protection Act. Training requirements include six hours for CISOs, three for other executives, nine for IT staff, and at least six for other employees. The results must be reported to the Korean Internet and Security Agency (Ministry of Science and ICT).

Second, regular and ad hoc security audits and other self-inspection activities are conducted by executives, such as the CEO or CISO. These activities serve as the basis for recognition as a self-regulated security company by government authorities, such as the Financial Supervisory Service. From the company's perspective, this provides an opportunity to maintain internal security management while enhancing its external image as a security-conscious company.

Third, the activities of the Information Security Committee include reviewing and deciding on major security management actions. These actions involve the introduction of IT security equipment and disciplinary measures for security violations. This serves as the basis for external auditors to assess a company's security management level during ISMS certification or major audits.

These provide non-financial benefits, such as an enhanced external reputation, and offer managers valuable insights into internal security management through the Information Security Committee. This is a proactive security management activity that enables the swift resolution of security vulnerabilities and control of future risks through rapid decision-making [24].

Previous studies have supported the positive impact of internal security management activities on corporate performance. Son (2015) argued that managerial, technical, and physical security activities lower costs, improve the external image, and support management goals [10]. Shin (2021) found that security training and internal processes promote innovation and enhance the performance of manufacturing firms [67]. Furthermore, Jeon (2020) and Jang (2020) demonstrated that various security incidents that occur when internal security management activities break down can cause significant damage to corporate performance [17,18].

Ultimately, internal security management activities are expected to have a positive impact on corporate performance. Therefore, this study proposes the following hypothesis:

Hypothesis 1: Internal security management activities have a positive impact on corporate performance.

2.2.2. External Security Management Activities and Corporate Performance

Companies may participate in external information security-related activities per the national security policies. These external activities include initiatives such as the Integrated Security Support Program for Critical Information and Communications Infrastructure. Another example is the Cyber Threat Information Analysis and Sharing System. Additionally, security threat response simulation exercises are hosted by agencies such as the Ministry of the Interior and Safety and the National Intelligence Service.

These activities go beyond mere participation in events or joining safety networks to prevent accidents. Collaborating with external security experts helps companies gain security insights and drive digital innovation [25]. Previous studies have reported that such external factors can lead to internal innovation and improved corporate performance [26,27].

Oh et al. (2024) explained that external factors can drive internal innovation linked to corporate performance. Similarly, Donaldson (2003) highlighted the innovative impact of external environmental conditions on organizations. Participation in external security activities helps institutions and companies demonstrate their IT security readiness. This, in turn, enhances the credibility of national security policy initiatives.

Thus, it is valuable to examine whether participation in external security management activities is driven by managerial intentions. It is also important to assess whether participation serves as an innovation factor that enhances corporate performance. Accordingly, this study proposes the following hypotheses:

 doi:10.20944/preprints202506.1578.v1

Hypothesis 2: External security management activities have a positive impact on corporate performance.

2.2.3. CISO's Work Independence and Corporate Performance

Under Article 45-3, Paragraph 3 of the Information and Communications Network Act, a CISO cannot perform other executive roles under certain conditions. In the case of financial institutions, specific regulations apply if total assets exceed 10 trillion won and the number of employees exceeds 1,000. According to the Electronic Financial Supervision Regulations, the CISO cannot hold the position of CIO in such cases.

A CISO is responsible for protecting IT systems and critical data from internal and external threats. However, if they are involved in developing and operating these systems, they may prioritize the interests of the CEO or shareholders over security. This could harm the interests of customers, business partners, and other stakeholders.

However, this may not apply to SMEs with agile cultures or to those unable to appoint a separate CISO due to their organizational characteristics. Some companies may expect greater operational efficiency if the CISO serves as a CIO or works within other technical departments. This efficiency may outweigh the security benefits of maintaining CISO's operational independence [13,23].

Examining differences in CISO operations as innovation factors influencing performance is supported by prior studies on organizational structure innovation [26,27,28]. This implies that changes in the internal organizational structure during the process of adapting to situational changes can enhance organizational efficiency and productivity.

Thus, the status and role of the CISO are becoming increasingly important [30]. Security management outcomes achieved through independent operations can positively impact corporate performance through organizational efficiency and an enhanced external image [10,28,30].

For small and medium-sized ventures, combining the CISO and CIO roles is often necessary due to limited resources. Technology-focused companies may also prefer this structure, based on their organizational characteristics. It is important to assess whether this approach effectively drives organizational innovation from a managerial perspective [30,41]. Therefore, this study proposes the following hypotheses:

Hypothesis 3: Having the CISO perform duties independently will have a positive impact on corporate performance.

Hypothesis 4: Having the CISO also serve as CIO will have a positive impact on corporate performance.

2.3. Financial Security Management Activities

2.3.1. IT Investment Activities and Corporate Performance

Despite the IT Productivity Paradox [31], many researchers consider IT infrastructure an important innovation resource and strategic factor in corporate management [32,33]. The average IT investment ratio in Korea is 2%, which varies by industry: 1.5% in agriculture, 2.2% in manufacturing and finance, and 5.9% in information and communications, with some telecommunications firms exceeding 10% [34,35].

The digital business environment stimulates investment in the information technology (IT) sector, making it a strategic priority for companies. After the 2011 Nonghyup hacking incident, the government advised financial firms to allocate at least 5% of their staff to IT roles and invest 7% of their IT budgets in information security. [29].

Considering industry and company characteristics, investment ratios may differ depending on IT informatization requirements. However, given that 70% of the annual IT budget is allocated to personnel costs, an investment ratio of 3–5% of a company's revenue is appropriate [36,37,38].

 doi:10.20944/preprints202506.1578.v1

Ultimately, government regulations and market competition continue to drive IT demand [20,37], supporting corporate growth [19,42]. Thus, the following research hypothesis is established:

Hypothesis 5: A higher investment ratio in the IT information technology sector will have a positive effect on corporate performance.

2.3.2. Information Security Sector Investment Activities and Corporate Performance

The information security sector faces emerging IT threats such as quantum computing, cloud growth, and artificial intelligence (AI), which require ongoing security upgrades that often overlap with those of broader IT system investments. [39,40]. Ultimately, managers must ensure that the IT and security departments work together through integrated IT governance to achieve business goals [39].

Previous studies suggest that adopting IT security technologies is an innovation that positively influences corporate performance [22,43,82]. Research shows that investments in information security can boost corporate performance, reflecting growing expectations for new technology adoption [82].

However, the investment ratio between the two sectors may vary depending on the business environment, and managers may make strategic choices appropriate to the situation. Managers make important decisions from a security management perspective [81]. Managers may decide to focus on investments in the information security sector, such as the introduction of security technology, and allocate relatively more resources.

This decision is based on the expectation that the anticipated benefits of information security investments outweigh the temporary costs incurred. Therefore, this study proposes the following hypothesis:

Hypothesis 6: A higher proportion of investment in the information security sector will have a positive effect on corporate performance.

2.4. ISMS (Information Security Management System) Certification System

2.4.1. System Description

The British Standards Institution (BSI) introduced the ISMS concept through ISO (International Organization for Standardization) /IEC (International Electrotechnical Commission) 27001 in 2005. Since then, public institutions and companies have adopted certification as an international standard for systematic information security management [21,44,45,46].

In Korea, it was introduced in 2011, and the personal information protection sector was integrated in 2018, establishing the ISMS-P (Information Security Management System-Personal) certification system [45,46,47].

Notably, ISMS certification is used not only by private companies but also by public national institutions. For Critical Information Infrastructure Protection (CIIP), agencies such as the National Intelligence Service and the Ministry of Science and ICT apply a security-level management system. This evaluation system requires that the ISMS certification be operated and maintained for at least one year. Key areas include administration, broadcasting and communications, finance, energy, construction and transportation, social welfare, and insurance networks [47,48].

2.4.2. The Significance of the ISMS Certification System in Relation to Internal and External Security Management Activities and Corporate Performance

The ISMS certification system serves as an objective tool for measuring the outcomes of security-management activities. It allows the evaluation of both non-financial and financial security management activities based on management commitment. This assessment evaluates the effectiveness of these activities. It also examines their alignment with the company's management objectives, such as management systems, information handling, IT system protection, and customer protection.

 doi:10.20944/preprints202506.1578.v1

Identifying the role of information security management tools in linking internal and external security activities to corporate performance is crucial. This understanding can help companies focus on their management resources more effectively. [49,50,51].

Therefore, this study examines whether ISMS certification serves as a significant moderating variable. This study investigates the interaction effects between internal and external security management activities and corporate performance. Based on this, the following hypothesis is proposed:

Research Hypothesis 7-1

Obtaining or maintaining ISMS (P) and ISO/IEC certification will strengthen the positive effect of internal security management activities on corporate performance.

Research Hypothesis 7-2

Obtaining or maintaining ISMS (P) and ISO/IEC certification systems will strengthen the positive effect of external security management activities on corporate performance.

2.4.3. The Significance of ISMS Certification Systems in Relation to CISO Work Independence and Corporate Performance

The CISO uses the ISMS tool to assess security levels and advise top management, who can then address vulnerabilities and align security policies with business goals [17,28,45]. The ISMS objectively measures security levels and enhances efficiency, regardless of whether the CISO operates independently or concurrently serves as CIO or another executive [46]. If an organization aims to enhance its business performance by integrating its CIO role while ensuring security management, a careful strategy is required. In such cases, adopting an ISMS certification system can be an effective information security management tool [30,49].

Previous studies show that a CISO's independence or dual role with the CIO can positively impact performance depending on company traits and strategies [13,28,30]. Therefore, it is important to examine the interaction between ISMS certification and CISO's operational independence. This study sets the following research hypotheses based on variations in CISO operational structures:

Research Hypothesis 7-3

The acquisition or maintenance of ISMS(P) and ISO/IEC certification systems will strengthen the positive effects on corporate performance when the CISO performs duties independently without concurrent roles in other executive organizations.

Research Hypothesis 7-4

Obtaining or maintaining ISMS(P) and ISO/IEC certification will strengthen the positive effect on corporate performance when the CISO concurrently serves as the CIO, overseeing the IT organization.

2.4.4. The Significance of ISMS Certification in Relation to the Proportion of Investment in IT and Information Security and Corporate Performance

It has become difficult for companies to supply products and services without relying on IT. Depending on the company's characteristics or strategy, investments in security equipment or personnel may need to be increased. A representative industry is the financial sector [29].

Security equipment, personnel, and new technologies are part of IT systems and are closely tied to customer-facing products and services. Therefore, investment in both areas is essential to maintain corporate performance [19,32]. Technology adoption and IT system competitiveness for agile market responses are the key drivers of corporate competitiveness [33,80,82].

Competitiveness is linked directly to corporate performance. Production activities that use IT platforms are not limited to the IT industry. IT platforms serve as important management tools even in traditional manufacturing and other non-IT industries. They are essential not only for customer-facing activities but also for internal management [38].

From a security management perspective, the following key questions arise: Should continuous investment in the broader IT sector be prioritized? Alternatively, should concentrated investments in the information security sector take precedence?

 doi:10.20944/preprints202506.1578.v1

Therefore, it is important to examine how an ISMS influences the impact of investment in these areas on corporate performance. Thus, the following research hypotheses are established:

Research Hypothesis 7-5

ISMS(P), obtaining or maintaining ISO/IEC certification will strengthen the positive effect on corporate performance as the investment ratio in the IT information technology sector increases.

Research Hypothesis 7-6

ISMS(P), obtaining or maintaining ISO/IEC certification will strengthen the positive effect on corporate performance as the investment ratio in the information security sector increases.

3. Materials and Methods

3.1. Research Model

This study aims to examine the relationship between corporate security management activities and corporate performance, as illustrated in Figure 1. It also aims to examine the moderating effect of information security management tools, such as the ISMS. Six independent variables and four control variables were defined to reflect differences in the general characteristics of the research sample. Additionally, two dependent variables—sales and operating profit—were identified to measure corporate performance.

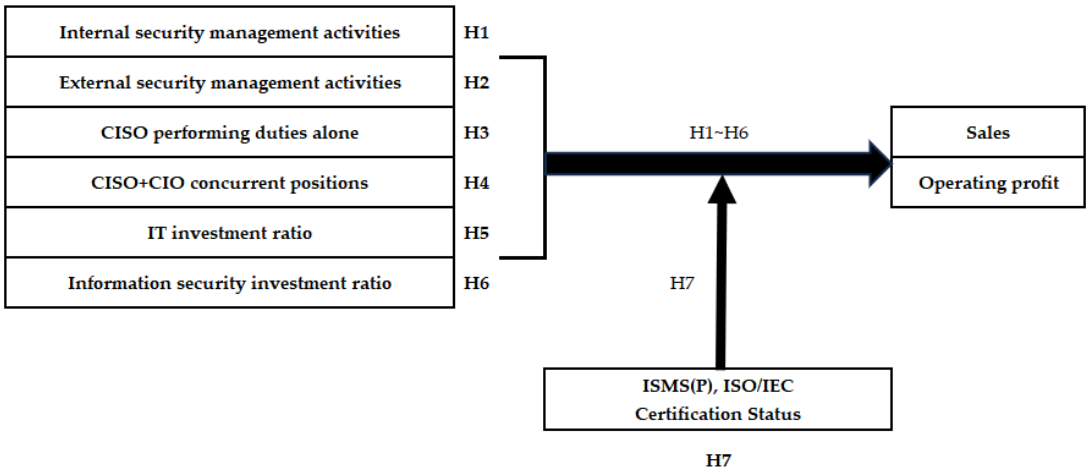

Figure 1. Research Model.

3.2. Variables

This study measured the impact of corporate security management activities on corporate performance, focusing on managers. Unlike previous studies, this study identifies both non-financial and financial information security activities within managerial decision-making processes. Research variables were defined for this study based on previous studies. Table 1 lists the contents of the independent variables.

Table 1. Independent Variables.

 doi:10.20944/preprints202506.1578.v1

Research Variables		Operational Definition	Measurement Method	References
Independent Variables	Internal Security Management Activities	2024 Information Security Activities Disclosure Contents ① Implemented information security training for all employees, ② Established an information security committee or ③ whether an internal information security audit was conducted	If one or more of ①, ②, or ③ were implemented, dummy 1; if no implementation was conducted, dummy 0	Jeon, S. J. (2020) [17]. Jang, S. S. (2020) [18]. Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013) [24].
	External Security Management Activities	2024 Disclosure Contents National-level security events ① Participated in the Integrated Security Support Project ② Participated in the Cyber Threat Information (C-TAS), or ③ Participated in security threat simulation exercises (KISA)	If one or more of ①, ②, or ③ were implemented, enter dummy 1; if none were implemented, enter dummy 0	Ahyun Kim, Yong Jin Kim. (2021) [25]. Garavan, T., & O'Brien, F. (2024) [26]. Lex Donaldson. (2003) [27].
	CISO performing duties independently	As of the end of June 2024, based on information disclosed CISO performing duties independently	If sole responsibility, dummy 1; if concurrent roles, dummy 0	Ciekanowski, M., Żurawski, S., Ciekanowski, Z., Pauliuchuk, Y., & Czech, A. (2024) [28]. Choi, D., & Kim, T. (2024) [30].
	CISO+CIO concurrent positions	As of the end of June 2024, based on information disclosed CISO concurrent positions with CIO	If concurrently performing CIO duties, dummy 1 Otherwise, dummy 0	Kim Kyung-hee. (2024) [13]. Oh Seok-hong, Son Tae-won, Lee Chang-gil. (2024) [22]. Julien Vehent. (2018) [23].
	IT Information Technology Sector Investment Ratio	Average sales from 2022 to 2024, the effective disclosure period, compared to the average IT information technology sector investment performance over three years	1 if 3% or more If less than 3%, dummy 0	Sun, J., & Jiao, H. (2024) [32]. Agustina, N., & Pramana, S. (2019) [33]. Gartner. (2024) [34]. Information and Communications Policy Research Institute. (2024) [35].
	Information Security Sector Investment Ratio	Effective Disclosure Period 2022–2024 IT Information Technology Sector Average Investment Amount Ratio 3-Year Average Information Security Sector Investment Execution Performance	8% or higher: dummy 1 If less than 8%, dummy 0	Lee Seung-min, Shin Ki-yoon, & Lee Jung-dong. (2022) [19]. Electronic Financial Supervision Regulations. (2011) [29]. Sharifuddin, N., & Mohamed, A. (2020, March) [39]. Rudner, M. (2013) [40].

Table 2 presents the moderating and dependent variables to be tested, along with the independent and control variables, all of which were included simultaneously. Moderating variables, such as ISMS(P) and ISO/IEC certification status, are dummy variables. The control variables, reflecting general company characteristics, are dummy variables, similar to the independent variables. By contrast, the dependent variables, sales and operating profit, are continuous variables.

Table 2. Moderating variables, dependent variables, and control variables.

Research Variables		Operational Definition	Measurement Method	References
Moderating variables	ISMS(P), ISO/IEC possession	Valid disclosure period 2022-2024 ① ISMS(P) or ② ISO 27001 certification acquisition/renewal maintenance status	①,② Among If one or more are met, dummy 1 Otherwise, dummy 0	Humphreys, E. (2016) [21]. Broderick, J. S. (2006) [44]. Song Ho-yeol, Lee Yong-joon, & Kang Jang-mok. (2024) [45]. Hong Seong-wook, & Park Jae-pyo. (2020) [46].
Dependent Variable	Sales, Operating Profit	Average Performance from 2022 to 2024	Public Institutions or Financial Institutions Survey Data (Continuous)	Go Byung-wook, & Kim Sung-tae. (2023) [53]. Science and Technology Policy Institute. (2023) [54]. Kim Jung-ho. (2023) [55]. Lee Kyu-jin. (2011) [56]. Moon Seon-woong. (2024) [57]. Kim Hyun-joo. (2023) [58]. Korea Credit Guarantee Fund. (2023) [59].
Control Variables	IT Industry group status	Based on disclosure content registered as of the end of June 2024 Corporate Industry Classification	IT industry group: dummy 1 Non-IT industry group: dummy 0	Information and Communications Policy Research Institute. (2024) [35]. Korea Institute of Science and Technology Evaluation and Planning. (2024) [36]. Li, X., Zhao, L., Ren, J., Sun, Y., Tan, C. F., Yeo, Z., & Xiao, G. (2024, December) [64].
	Industry Classification	Based on disclosure content registered as of the end of June 2024 Corporate Industry Classification	Manufacturing industry: Dummy 1 Service industry: Dummy 0	Korean Standard Industrial Classification (2024) [65]. Kakushadze, Z., & Yu, W. (2017) [66]. Shin Eun-hee. (2021) [67]. Lee Heung-bae. (2022) [68].
	Information Security Disclosure Type	Information security disclosure content as of the end of June 2024 Information security disclosure type classification	Dummy 1 for companies with disclosure obligations Dummy 0 for companies with voluntary disclosure	Kim Seon-ju, Kim Tae-seong. (2023) [69]. National Intelligence Service (2024) [70].
	Asset Size	Asset valuation amounts measured through surveys of public institutions or financial institutions from 2022 to 2024	2 trillion KRW to 5 trillion KRW is dummy 1 0.3 trillion KRW to 2 trillion KRW is dummy 0	Kim Sang-cheol, & Park Yong-soo. (2022) [71]. Lim Ji-young, & Han Jun. (2022) [72]. Rizka, N. R., & Ulfida, D. (2024) [73]. Rahima, A. Y., & Muid, D. (2023) [74]. Utami, S. W. (2023) [75]. Fiana, F., & Endri, E. (2025) [76].
		Asset valuation amounts measured through surveys of public institutions or financial institutions from 2022 to 2024	1 if 5 trillion KRW or more 0.3 trillion KRW to 2 trillion KRW is 0	

3.3. Analysis Method

In the first stage of the research analysis, a multiple regression analysis was conducted on the independent and control variables. In this study, the two dependent variables were analyzed separately, and the significance of the results was assessed. In other words, changes in sales (a growth indicator) and operating profit (a profitability indicator) were compared from the perspective of security management strategies.

Multiple regression analysis helps identify the relative magnitude and direction of each independent variable's influence on the dependent variable. It also reveals the interactions between

 doi:10.20944/preprints202506.1578.v1

the independent variables. This approach facilitates the analysis of complex and realistic research problems.

In particular, it is effective in confirming the pure influence of the main independent variable when the control variables that require control are included. For this purpose, IBM SPSS ver 30.0 was utilized [60,61,62].

In the second stage of the analysis, the presence or absence of an ISMS certification system was defined as a moderating variable. This study examined how the interaction between each independent variable and the moderating variable affected the dependent variables. As in multiple regression analysis, both dependent variables were verified using the same control variables for each independent variable. For this purpose, we used the Process macro ver 4.2 (Model 1) proposed by Hayes (2013) [16,63].

The statistical significance of the estimated regression coefficients was evaluated by considering the characteristics of the sample companies and the research objectives. Bootstrapping was conducted 5,000 times with a significant level set at 0.1. The 90% confidence intervals (LLCI and ULCI) were checked to determine whether they included zero.

3.4. Data Collection

Data on the sample companies were obtained from the "Information Security Disclosure Status" section of the Information Security Disclosure Comprehensive Portal (isds.kisa.or.kr). This portal is operated by the Korean Internet and Security Agency under the Ministry of Science and ICT. The dataset targeted 545 companies that disclosed their information between 2022 and 2024. The financial data for each company were obtained from the statistical data of the Samsung Securities Research Center.

One general characteristic of the sample companies is the "mandatory/voluntary" disclosure classification under an information security disclosure system. According to Article 13 of the Act on the Promotion of the Information Security Industry, companies that meet certain criteria are subject to mandatory reporting. These criteria include business sector, company revenue, and number of users. Such companies are required to report to the Korean Internet and Security Agency, a government-affiliated body.

By contrast, voluntary disclosure is available to all businesses that operate through information and communication networks. However, both mandatory and voluntary reporters must submit reports to the disclosure portal by June 30 of each year. Thus, the information security disclosure systems have a regulatory nature. This provides evidence that the research data obtained are objective and credible.

First, frequency analysis was conducted to understand the general characteristics of the research sample. The four variables representing the general characteristics of the research participants were disclosure type(voluntary or mandatory), industry type, IT industry status, and asset size. Table 3 lists the characteristics of the 545 companies in the research sample.

 doi:10.20944/preprints202506.1578.v1

Table 3. Characteristics of Research Subjects.

Characteristic	Category	Frequency (Number)	Percentage (%)
		545	100
Voluntary/Mandatory	Voluntary	41	7.5
	Mandatory	504	92.5
Industry	Service Industry	182	33.4
	Manufacturing Industry	363	66.6
IT Industry group status	Non-IT Industry	459	84.2
	IT Industry	86	15.8
Asset Size	300 billion KRW or more to less than 2 trillion KRW	369	67.7
	2 trillion KRW or more to less than 5 trillion KRW	78	14.3
	5 trillion KRW or more	98	18

By confirming the general characteristics of the research participants, we found differences in the ratios between the variables. Therefore, we dummy-coded these variables and used them as control variables in the regression analysis. We also performed descriptive statistical analyses of the independent, moderator, and dependent variables. First, we calculated the frequencies and ratios of the independent variables and moderator variables, which were categorical variables, and the results of the analysis are shown in Table 4.

Table 4. Descriptive statistical analysis of research variables (categorical variables).

Research variable	Category	Frequency (number)	Percentage (%)
		545	100
Internal Security Management Activities	Not implemented	423	77.6
	Implemented	122	22.4
External Security Management Activities	Not implemented	463	85
	Implemented	82	15
CISO performing duties independently	No	433	79.4
	Yes	112	20.6
CISO+CIO concurrent positions	No	453	83.1
	Yes	92	16.9
IT Information Technology Sector Investment Ratio	Less than 3%	468	85.9
	3% or more	77	14.1
Information Security Sector Investment Ratio	Less than 8%	328	60.2
	8% or more	217	39.8
ISMS(P), ISO/IEC possession	Not certified	337	61.8
	Certified	208	38.2

Next, we calculated the mean and standard deviation of the dependent variable, which was continuous. We then analyzed the skewness and kurtosis to assess whether the assumption of normality was satisfied. The assumption was considered met when the absolute value of skewness

 doi:10.20944/preprints202506.1578.v1

was less than 2 and the absolute value of kurtosis was less than 7, indicating that the data approximated a normal distribution [52]. The detailed analysis results are presented in Table 5.

Table 5. Descriptive statistics analysis of dependent variables.

	N	Minimum value	Maximum value	Average	Standard deviation	Skewness	Kurtosis
Sales (100 million KRW)	545	23.13	3058374.17	47085.4145	180592.4621	11.084	159.028
ln_Sales (100 million KRW)	545.000	3.140	14.930	9.341	1.505	.194	1.851
Operating profit (100 million KRW)	545.000	.860	378,114.710	3,634.744	21,247.921	13.569	209.631
ln_Operating profit (100 million KRW)	545.000	-.150	12.840	6.289	1.796	.013	0.876

The results of checking the skewness and kurtosis of sales and operating income, which measured as dependent variables, indicated that the normality assumption was not met. Therefore, in the actual research analysis, the data were transformed using a natural logarithm (ln). After applying a natural logarithm transformation, the skewness of sales and operating profits ranges from 0.013 to 0.194, satisfying the criterion of less than 2. The kurtosis ranged from 0.876 to 1.851, meeting the criterion of less than 7, thereby fulfilling the assumption of a normal data distribution [52].

Among the performance measurement indicators for corporate management, sales revenue is a widely used growth indicator. Sales revenue analysis is used to evaluate growth potential, innovation capacity, and the effectiveness of support policies of industries and companies [53,54,55]. Additionally, operating profit was used as an indicator to assess the quality of corporate growth, specifically profitability and sales revenue.

It is calculated by subtracting general administrative expenses, such as sales and labor costs, from the gross profit generated during the fiscal year. Operating profit is considered to be the performance metric most faithful to a company's fundamental business objectives [56]. It is widely used to measure performance in core areas of business management, such as R&D outcomes and financial analysis [57,58,59]. In this study, revenue and operating profit are used as dependent variables to verify the impact of security management activities on corporate performance.

4. Results

4.1. Verification Results of Research Hypotheses H1–H6

Table 6 presents the results of multiple regression analysis of sales revenue. First, in the analysis of the control variables related to a company's general characteristics, differences in autonomy/obligation, IT industry classification, and asset size were statistically significant. The analysis shows that companies with mandatory information security disclosure and those with larger asset sizes exhibit a positive (+) effect on sales revenue.

Among the independent variables, both internal and external security management activities had a statistically significant positive (+) effect. The other variables exhibited negative (-) effects. However, the results of the CISO + CIO dual role and IT investment ratio were also statistically significant, indicating research relevance despite the direction of the effect. Although the positive (+) effects were not confirmed, the observed negative (-) effects were statistically significant.

Based on the verification of the research hypotheses regarding sales revenue, H1 and H2 were accepted, while H3 through H6 were rejected.

Table 7 presents the results of the multiple regression analysis of the operating profit. Unlike with sales, the effect of the control variables was not statistically significant for IT industry classification. However, similar to the sales results, autonomy/obligation and asset size showed statistically significant correlations. Mandatory disclosure and larger asset size had a positive effect on operating profit, consistent with the sales findings.

 doi:10.20944/preprints202506.1578.v1

The analysis of independent variables revealed that all were either statistically insignificant or showed effects contrary to the research hypotheses. However, similar to the sales analysis, the CISO + CIO dual role and IT investment ratio had statistically negative effects, contrary to the research hypotheses. These contrary effects differences were statistically significant.

These findings diverge from the conventional expectations, as was also observed in the sales results. This suggests that managers should adopt flexible security strategies tailored to their company's characteristics and market conditions.

The results of the hypothesis testing for operating profit showed that H1 through H6 were rejected.

Table 6. Relationship analysis of the impact of security management activities on sales revenue.

	Research Variable	B	β	SE	t	p	LLCI	ULCI
Control Variables	(constant)	7.999		.178	44.888***	.000	7.705	8.292
	Voluntary/Mandatory	.922	.162	.145	6.368***	.000	.684	1.161
	Industry	-.040	-.013	.100	-.401	.688	-.204	.124
	IT Industry group status	-.320	-.078	.147	-2.180*	.030	-.561	-.078
	Asset size (2 trillion KRW or more but less than 5 trillion KRW = 1)	1.207	.281	.107	11.320***	.000	1.032	1.383
	Asset size (5 trillion KRW or more = 1)	2.805	.717	.102	27.464***	.000	2.637	2.974
Independent Variables	Internal Security Management Activities	.327	.217	.094	3.471**	.001	.172	.482
	External Security Management Activities	.262	.062	.110	2.379*	.018	.081	.444
	CISO performing duties independently	-.042	-.011	.092	-.455	.650	-.194	.110
	CISO+CIO concurrent positions	-.191	-.048	.100	-1.919+	.056	-.355	-.027
	IT Information Technology Sector Investment Ratio	-1.115	-.258	.148	-7.543***	.000	-1.359	-.872
	Information Security Sector Investment Ratio	-.063	-.020	.075	-.830	.407	-.187	.062
							F=112.275*** (p<.001); R^2 = .699	

Note 1. + p<0.10, * p<.05, ** p<.01, *** p<.001

Note 2. dependent variable : ln_Sales

Table 7. Relationship analysis of the impact of security management activities on operating profit.

	Research Variable	B	β	SE	t	p	LLCI	ULCI
Control Variables	(constant)	5.204		.269	19.350***	.000	4.761	5.647
	Voluntary/Mandatory	.418	.061	.219	1.911+	.057	.058	.778
	Industry	.031	.008	.150	.205	.837	-.217	.279
	IT Industry group status	-.027	-.005	.221	-.122	.903	-.392	.338
	Asset size (2 trillion KRW or more but less than 5 trillion KRW = 1)	1.505	.294	.161	9.354***	.000	1.240	1.771
	Asset size (5 trillion KRW or more = 1)	3.114	.666	.154	20.198***	.000	2.860	3.368
Independent Variables	Internal Security Management Activities	.171	.095	.142	1.201	.230	-.063	.405
	External Security Management Activities	.164	.033	.166	.988	.324	-.110	.439
	CISO performing duties independently	-.055	-.012	.139	-.394	.693	-.284	.174
	CISO+CIO concurrent positions	-.258	-.054	.150	-1.716+	.087	-.505	-.010
	IT Information Technology Sector Investment Ratio	-.810	-.157	.223	-3.629***	.000	-1.178	-.442
	Information Security Sector Investment Ratio	.036	.010	.114	.314	.754	-.152	.223
							F=52.080*** (p<.001); R^2 = .518	

 doi:10.20944/preprints202506.1578.v1

Note 1. + p<0.10, * p<.05, ** p<.01, *** p<.001

Note 2. dependent variable : ln_Operating profit

4.2. Results of the Moderating Effect Analysis for Research Hypothesis H7

4.2.1. Analysis of the Moderating Effects of ISMS (P) and ISO/IEC Certification Status on the Relationship Between Security Management Activities and Sales Revenue

Table 8 presents the results of the moderating effect analysis of the ISMS (P) and ISO/IEC certification system ownership on the relationship between security management activities and sales revenue. Unlike the previous multiple regression analysis, the independent variables were analyzed individually along with the control variables. Therefore, the findings for the same research variables varied slightly due to changes in the analytical model.

Table 8.

	Research Variable	Internal Security Management Activities		External Security Management Activities		CISO performing duties independently		CISO+CIO concurrent positions		IT Information Technology Sector Investment Ratio		Information Security Sector Investment Ratio	
		B	p	B	p	B	p	B	p	B	p	B	p
Control Variables	(constant)	7.664***	.000	7.691***	.000	7.730***	.000	7.773***	.000	7.900***	.000	7.682***	.000
	Voluntary/Mandatory	0.990***	.000	0.995***	.000	0.987***	.000	0.969***	.000	0.993***	.000	0.983***	.000
	Industry	.141	.175	.132	.202	.142	.170	.094	.365	-.045	.647	.137	.187
	IT Industry group status	-.837***	.000	-.838***	.000	-.835***	.000	-.886***	.000	-.310*	.031	-.833***	.000
	Asset size (2 trillion KRW or more but less than 5 trillion KRW = 1)	1.293***	.000	1.3***	.000	1.302***	.000	1.310***	.000	1.199***	.000	1.307***	.000
	Asset size (5 trillion KRW or more = 1)	2.972***	.000	2.977***	.000	2.977***	.000	2.934***	.000	2.759***	.000	2.980***	.000
	Independent Variable (X)	0.312*	.048	.059	.707	-.196	.129	-.080	.510	-2.340***	.000	.053	.586
Moderating variable	ISMS(P), ISO/IEC possession(W)	.132	.217	.125	.204	.042	.677	0.185+	.061	0.248**	.009	.172	.122
	Interaction Term (XW)	-.254	.206	-.052	.811	0.373*	.049	-.468*	.034	1.364***	.000	-.141	.382
	Model Fit	$F=132.286^{***}$ (p<.001); R^2 = .664		$F=130.804^{***}$ (p<.001); R^2 = .661		$F=132.214^{***}$ (p<.001); R^2 = .664		$F=134.163^{***}$ (p<.001); R^2 = .667		$F=162.319^{***}$ (p<.001); R^2 = .708		$F=131.033^{***}$ (p<.001); R^2 = .662	

Note 1. + p<0.10, * p<.05, ** p<.01, *** p<.001

Note 2. dependent variable : ln_Sales

For the control variables, the same results were observed as those in the multiple regression analysis. The differences in autonomy/obligation, IT industry sector, and asset size are statistically significant for all six independent variables. Mandatory information security disclosure and larger asset size had a positive effect on sales revenue. In contrast, a negative effect was observed in the IT industry.

First, the F-test and R-squared (R^2) values were examined to confirm the model fit for each independent variable. All six independent variables were statistically significant at the .001 level, with appropriate explanatory power. In particular, the R-squared (R^2) statistic for the IT sector investment ratio is the highest at .708. All six regression models were statistically significant.

Individual regression coefficients were used to test the hypotheses based on the validated regression models. Internal security management activities (B = .312) had a statistically significant positive (+) effect at a .05 significance level. Companies that implement internal security management are expected to have higher sales than those that do not.

However, the interaction term with the moderating variable was not statistically significant. Therefore, the presence or absence of ISMS (P) and ISO/IEC certification does not moderate this relationship.

 doi:10.20944/preprints202506.1578.v1

External security management activities are not statistically significant. In other words, they are expected to be unrelated to the sales revenue. Furthermore, the interaction term was also not statistically significant, confirming the absence of a moderating effect.

CISO's sole responsibility was not statistically significant, but the interaction term with the moderator variable (B = .373) was statistically significant at the .05 level. In Hayes' (2017) process macro-analysis, the moderating effect in the research model is acknowledged if the effect of the interaction model is acknowledged [77,78,79]. In other words, the CISO alone is not a significant factor in influencing sales revenue. However, possessing ISMS(P) and ISO/IEC certifications is expected to have a reinforcing effect that positively moderates this relationship.

Further analysis is needed to understand how the interaction term, which was statistically significant, manifests itself. Therefore, the participants were divided into certified and non-certified groups. Significance was re-confirmed using a 90% confidence interval (LLCI, ULCI) from 5,000 bootstrapping iterations. Table 9 presents the results of the analysis.

Table 9.

Moderating variable	B	SE	t	p	Bootstapping CI	
					LLCI	ULCI
ISMS(P), ISO/IEC Not certified	-.196	.129	-1.519	.129	-.409	.017
ISMS(P), ISO/IEC Certified	.177	.139	1.275	.203	-.052	.405

* p<.05, ** p<.01, *** p<.001.

The results showed that the effect of the CISO's sole performance on sales revenue was relatively higher in companies that held ISMS (P) and ISO/IEC (B = .177) than in those that did not (B = -.196). However, the regression coefficients for all groups were not statistically significant because 0 was included in the 90% confidence interval of the bootstrapping method.

In other words, the moderating variable strengthens the relationship between the independent and dependent variables. However, because the influence of the independent variable was not significant, the effect could not be interpreted clearly [63, 79]. Figure 2 presents the results of the analysis.

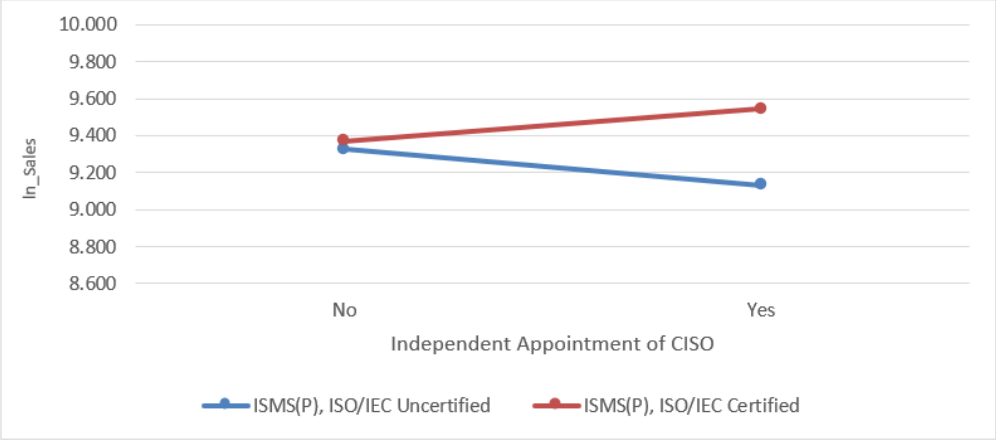

Figure 2. Influence of ISMS(P), ISO/IEC possession status on the correlation between CISO's independent work performance and sales amount.

The CISO + CIO dual responsibility was not statistically significant. In other words, the dual roles of the CISO + CIO and sales revenue are expected to be unrelated. However, the interaction term (B=-0.468) was statistically significant at the .05 level. That is, the dual role of the CISO + CIO is

 doi:10.20944/preprints202506.1578.v1

not a variable that significantly affects sales revenue. However, the presence or absence of an ISMS(P) and ISO/IEC certification was found to have reinforcing effects in the same direction (negative).

Additionally, to confirm the significance of the interaction term, the sample group was divided based on the possession of certification systems. Bootstrapping was then performed 5,000 times to verify significance using a 90% confidence interval (LLCI, ULCI). Table 10 presents the results of this analysis.

Table 10. Moderating effect analysis of ISMS (P), ISO/IEC certification status on the relationship between the impact of CISO+CIO dual roles on sales revenue (Bootstrapping method).

Moderating variable	B	SE	t	p	Bootstapping CI	
					LLCI	ULCI
ISMS(P), ISO/IEC Not certified	-.080	.121	-.659	.510	-.279	.120
ISMS(P), ISO/IEC Certified	-.548	.184	-2.971**	.003	-.852	-.244

* p<.05, ** p<.01, *** p<.001.

The results show that companies with ISMS (P) and ISO/IEC (B = -0.548) had a greater relative impact than companies without them (B = -0.080). Furthermore, the regression coefficient of the group holding ISMS(P) and ISO/IEC was statistically significant, as it did not include zero within the 90% confidence interval of bootstrapping. Thus, the moderating variable strengthens the negative relationship between the independent and dependent variables. Although the directionality differs from the research hypotheses, it is significant. Figure 3 illustrates the results.

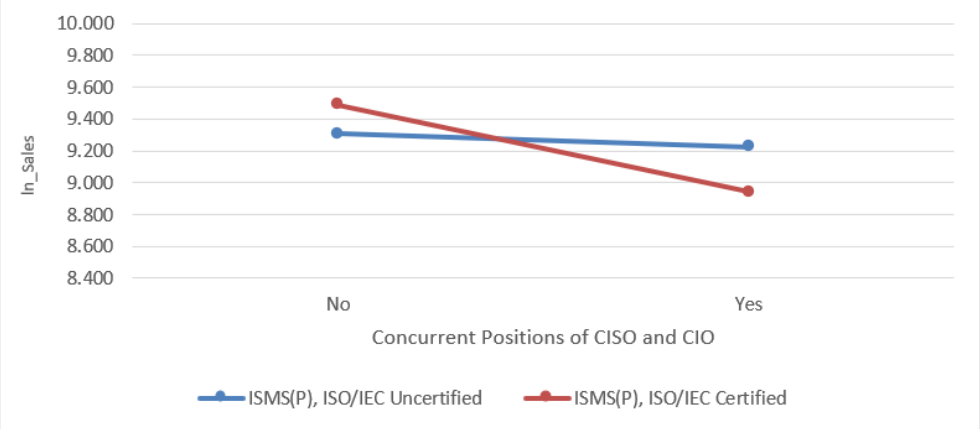

Figure 3. Influence of ISMS (P), ISO/IEC certification on the correlation between CISO+CIO dual roles and sales revenue.

The proportion of investment in the IT sector (B = -2.340) had a statistically significant negative effect at the 0.001 level. Companies with an IT sector investment ratio of 3% or more relative to sales were expected to have lower sales than those with a lower ratio. Notably, the interaction term (B=1.364) was statistically significant at the .001 level.

In other words, the IT investment ratio had a significantly negative impact on sales. However, the presence or absence of ISMS(P) and ISO/IEC certification moderated this effect, reversing the relationship in a positive direction. Additionally, to confirm the significance of interaction term, the sample was divided, and 5,000 bootstrap resamples were conducted to generate 90% confidence intervals (LLCI and ULCI). Table 11 presents the results of this analysis.

 doi:10.20944/preprints202506.1578.v1

Table 11. Analysis of the moderating effects of ISMS (P), ISO/IEC certification status on the relationship between IT investment ratio and sales revenue (Bootstrapping method).

Moderating variable	B	SE	t	p	Bootstapping CI	
					LLCI	ULCI
ISMS(P), ISO/IEC Not certified	-2.340	.294	7.963***	.000	-2.824	-1.856
ISMS(P), ISO/IEC Certified	-.975	.158	6.164***	.000	-1.236	-.715

* p<.05, ** p<.01, *** p<.001.

The results showed that companies with ISMS (P) and ISO/IEC certification (B = -0.975) experienced a less negative effect than companies without such certifications (B = -2.340). Additionally, the regression coefficients of the two groups were statistically significant because the bootstrapping 90% confidence interval did not include 0. This indicates that the moderating variable had a positive (+) effect on mitigating the relationship between the independent and dependent variables. Figure 4 illustrates the results.

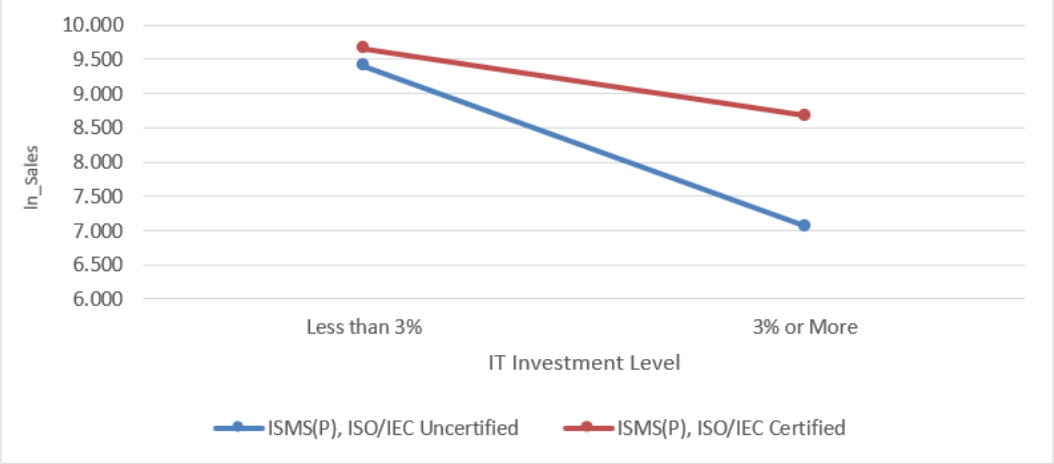

Figure 4. Influence of ISMS (P), ISO/IEC certification on the correlation between IT investment ratio and sales revenue.

The investment ratio in the information security sector, however, was not statistically significant. In other words, it did not appear to be related to sales. The interaction term is not statistically significant, confirming the absence of a moderating effect.

The results of the hypothesis testing for the moderating effect on sales showed that H7-3 and H7-5 were accepted, while H7-1, 2, 4, and 6 were rejected.

4.2.2. Analysis of the Moderating Effect of ISMS (P) and ISO/IEC Certification Status on the Relationship Between Security Management Activities and Operating Profit

Table 12 presents the results of the analysis of the moderating effects of ISMS (P) and ISO/IEC certification status on the relationship between security management activities and operating profits. The analysis was conducted in the same manner as for sales revenue.

Table 12. Analysis of the moderating effect of ISMS (P), ISO/IEC certification on the relationship between security management activities and Operating profit (Process Macro Model 1).

 doi:10.20944/preprints202506.1578.v1

	Research Variable	Internal Security Management Activities		External Security Management Activities		CISO performing duties independently		CISO+CIO concurrent positions		IT Information Technology Sector Investment Ratio		Information Security Sector Investment Ratio	
		B	p	B	p	B	p	B	p	B	p	B	p
Control Variables	(constant)	4.864***	.000	4.86***	.000	4.891***	.000	4.937***	.000	5.034***	.000	4.777***	.000
	Voluntary/Mandatory	0.487*	.024	0.486*	.027	0.485*	.024	0.476*	.027	0.494*	.019	0.503*	.021
	Industry	.229	.127	.229	.125	.238	.111	.199	.184	.072	.629	.230	.124
	IT Industry group status	-.441*	.024	-.439*	.025	-.437*	.024	-.419*	.014	.020	.925	-.430*	.027
	Asset size (2 trillion KRW or more but less than 5 trillion KRW = 1)	1.514***	.000	1.511***	.000	1.510***	.000	1.522***	.000	1.420***	.000	1.524***	.000
	Asset size (5 trillion KRW or more = 1)	3.128***	.000	3.127***	.000	3.125***	.000	3.091***	.000	2.936***	.000	3.134***	.000
	Independent Variable (X)	-.020	.931	.023	.918	-.213	.253	-.193	.271	-2.129***	.000	.154	.276
Moderating variable	ISMS(P), ISO/IEC possession(W)	0.306*	.049	0.308*	.030	.225	.122	0.328*	.022	0.407**	.005	0.380*	.018
	Interaction Term (XW)	.007	.982	-.038	.904	.381	.162	-.220	.490	1.292**	.005	-.198	.394
	Model Fit	$F=68.801^{***}$ ($p<.001$); $R^2=.507$		$F=68.801^{***}$ ($p<.001$); $R^2=.507$		$F=69.312^{***}$ ($p<.001$); $R^2=.508$		$F=69.708^{***}$ ($p<.001$); $R^2=.510$		$F=76.377^{***}$ ($p<.001$); $R^2=.533$		$F=69.115^{***}$ ($p<.001$); $R^2=.510$	

Note 1. + p<0.10, * p<.05, ** p<.01, *** p<.001. Note 2. dependent variable : ln_Operating profit.

The control variables yielded different results compared to the analysis of sales revenue. The statistical significance of the differences in autonomy/obligation and asset size remained the same. However, among the independent variables, only the IT investment ratio was not statistically significant. This specifically relates to whether the company belongs to the IT industry.

However, as in the sales revenue analysis, all independent variables show a positive (+) effect on operating profit as the information security disclosure method becomes more mandatory and asset size increases. Similar to the sales results, this indicates a consistent positive trend. However, no correlation was found between the operating profits across different industries.

The F-test and R-squared (R^2) values for all six independent variables were significant at the .001 level, confirming a good model fit and explanatory power. All six regression models were statistically significant. Hypothesis testing was performed by interpreting the individual regression coefficients based on the validated regression models.

Among the interaction terms between the six independent and moderator variables, only the IT sector investment ratio was statistically significant (B = 1.292, P < .01). The independent variable effect (B = -2.129) was also found to have a significant negative impact at the .001 significance level. This result is similar to the sales revenue findings. In other words, companies with an IT investment ratio of 3% or more relative to sales revenue are expected to have lower sales revenue than those without such an investment ratio.

However, it was confirmed that ISMS (P) and ISO/IEC certifications have a moderating effect that reverses this relationship to have a positive (+) effect on operating profit. Additionally, the significance of the interaction term was confirmed by dividing the sample group and conducting 5,000 bootstrapping runs to obtain 90% confidence intervals (LLCI and ULCI). Table 13 presents the results of this analysis.

Table 13. Analysis of the moderating effect of ISMS (P), ISO/IEC certification on the relationship between IT investment ratio and operating profit (Bootstrapping method).

 doi:10.20944/preprints202506.1578.v1

Moderating variable	B	SE	t	p	Bootstapping CI	
					LLCI	ULCI
ISMS(P), ISO/IEC Not certified	-2.129	.443	4.800***	.000	-2.860	-1.398
ISMS(P), ISO/IEC Certified	-.837	.239	3.505***	.000	-1.231	-.444

* p<.05, ** p<.01, *** p<.001.

Companies with ISMS(P) and ISO/IEC certification (B = -0.837) showed a relatively lower impact than companies without such certifications (B = -2.129). In addition, because the regression coefficients of the two groups did not include zero within the 90% confidence interval of bootstrapping, the results were statistically significant. In other words, the moderating variable had a positive (+) effect on mitigating the relationship between the independent and dependent variables. Figure 5 illustrates these results.

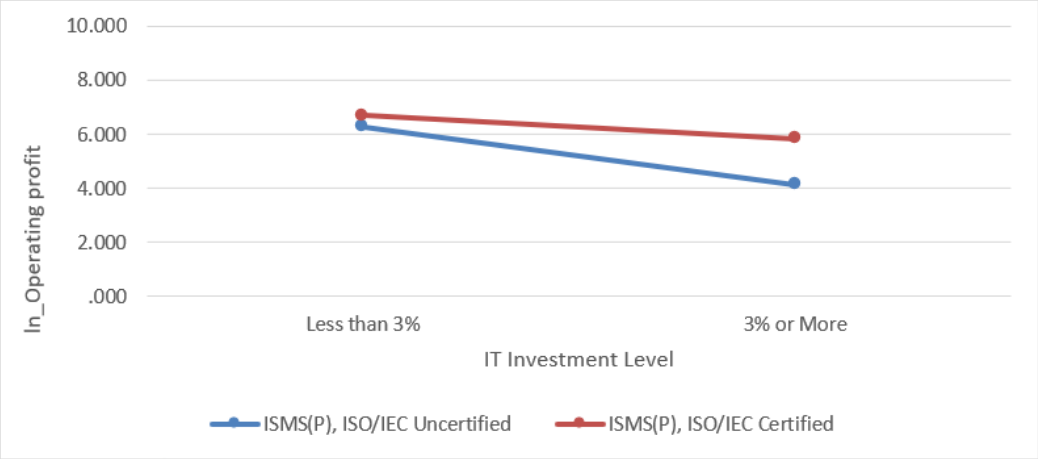

Figure 5. Influence of ISMS (P), ISO/IEC certification on the correlation between IT investment ratio and operating profit.

Among the moderating effects on operating profit, only H7-5 was accepted, whereas H7-1, 2, 3, 4, and 6 were rejected.

4.3. Summary Table of Research Hypothesis Verification Results

Table 14 summarizes the results of the verified research hypotheses. In the multiple regression analysis of sales, H1 and H2 were accepted. However, H4 and H5 were rejected because they showed results contrary to those of the research hypotheses, although both were statistically significant.

In the multiple regression analysis of operating profits, all research hypotheses were rejected. However, similar to sales revenue, H4 and H5 show results that are opposite to those of the research hypotheses, although they are also statistically significant.

In the moderating effect analysis of the ISMS (P) and ISO/IEC certification status on sales, H7-3 and H7-5 were adopted. However, H4 and the interaction term with the CISO + CIO dual role were rejected because they showed the opposite direction of the research hypothesis, but they were statistically significant.

In the moderating effect analysis of ISMS (P) and ISO/IEC certification status on operating profits, H7-5 was adopted.

 doi:10.20944/preprints202506.1578.v1

Table 14. Summary of research hypothesis verification results.

research hypothesis	verification results	
	Sales	Operating profit
Hypothesis 1: Internal security management activities have a positive impact on corporate performance.	Adopted	Rejected
Hypothesis 2: External security management activities have a positive impact on corporate performance.	Adopted	Rejected
Hypothesis 3: Having the CISO perform duties independently will have a positive impact on corporate performance.	Rejected	Rejected
Hypothesis 4: Having the CISO also serve as CIO will have a positive impact on corporate performance.	Rejected	Rejected
Hypothesis 5: A higher proportion of investment in IT will have a positive effect on corporate performance.	Rejected	Rejected
Hypothesis 6: A higher proportion of investment in information security will have a positive effect on corporate performance.	Rejected	Rejected
Hypothesis 7-1: Obtaining or maintaining ISMS(P) and ISO/IEC certification will strengthen the positive effect of internal security management activities on corporate performance.	Rejected	Rejected
Hypothesis 7-2: Obtaining or maintaining ISMS (P) and ISO/IEC certification will strengthen the positive effect of external security management activities on corporate performance.	Rejected	Rejected
Hypothesis 7-3: Obtaining or maintaining ISMS (P) and ISO/IEC certification will strengthen the positive effect on corporate performance when the CISO performs duties independently without concurrently serving in other executive organizations.	Adopted	Rejected
Hypothesis 7-4: Obtaining or maintaining ISMS(P) and ISO/IEC certification will strengthen the positive effects on corporate performance when the CISO concurrently serves as the CIO overseeing the IT technology information organization.	Rejected	Rejected
Hypothesis 7-5: Obtaining or maintaining ISMS(P) and ISO/IEC certification will strengthen the positive effects on corporate performance as the proportion of investment in the IT information technology sector increases.	Adopted	Adopted
Hypothesis 7-6: Obtaining or maintaining ISMS(P) and ISO/IEC certification will strengthen the positive effect on corporate performance as the proportion of investment in the information security sector increases.	Rejected	Rejected

5. Discussion

This study yielded five meaningful points for discussion.

First, although sales and operating profits share commonalities as dependent variables for verifying corporate performance, they are not identical. They produced different results in terms of independent and moderating variables and responses. This indicates that managers should adopt flexible strategic decisions when seeking to achieve management goals through security management activities.

Specifically, H1 (internal security management activities) and H2 (external security management activities) were adopted for sales, but were not supported for operating profits. This suggests that internal and external security management activities incur costs related to information security, which may negatively impact operating profits. However, the positive benefits gained from these activities, such as improved work efficiency and an enhanced external image, are relatively greater. As a result, the overall effect may be favorable for corporate performance.

Seo (2015) argues that corporate security activities can overcome cost issues arising from investment in management resources and improve operational efficiency and market competitiveness, ultimately increasing corporate profits [5]. Thus, corporate security activities should be accepted as part of an active management strategy.

Shin (2021) also confirmed that security activities in the manufacturing industry can lead to improved management performance by improving business processes in the production process [67]. Therefore, instead of focusing on the loss of management resources due to increased costs in the management sector caused by internal and external security management activities, a different perspective is required. It is important to consider that the benefits of corporate performance may also be greater.

Second, the perception that security management activities lead only to unnecessary investments in information security or increased management costs should be discarded. These activities should not be viewed as obstacles to management. Instead, they should be accepted as essential elements of management innovation.

 doi:10.20944/preprints202506.1578.v1

Specifically, we did not confirm whether H7-3, the sole responsibility of the CISO, had any impact on sales. However, the interaction with information security management tools was found to have a statistically significant positive effect. This suggests a moderating role of these tools in enhancing relationships. This can be accepted as an example of how strict security management activities can act as innovation factors.

In addition, in a multiple regression analysis of the control variables, companies obligated to disclose information security showed a statistically significant positive effect on corporate performance. This is in comparison with companies that voluntarily disclose. These results further support this hypothesis.

Furthermore, Byun (2019) stated that personal information protection activities regulated by legal systems can enhance the competitiveness of IT companies [11]. Jung (2007) argued that government regulations paradoxically stimulate technological innovation in companies [12]. This demonstrates that information security, although regulated, has broader implications. It can also act as an innovative element that enhances corporate competitiveness through the improved operational efficiency resulting from regulatory compliance.

Third, in a growth-oriented management structure requiring significant strategic investment in IT, short-term financial performance may not fully reflect the benefits of security management activities. It is important to recognize that such benefits may take time to materialize. The results of multiple regression analysis of the control variables support this view. They showed that the positive effect on corporate performance is more pronounced in manufacturing industries and companies with larger asset sizes, whereas the negative effect is more noticeable in the IT industry.

Additionally, in the multiple regression analysis of the independent variables, H4 (when the CISO and CIO are combined) and H5 (when the investment ratio in the IT sector increases) also show a significant negative impact. In other words, management activities such as combining the CIO's role with IT system operations or increasing direct investment levels in the IT sector have a negative impact on financial performance.

Contrary to the findings of this study, Alharbi and Gregg (2022) and Mithas and Rust (2016) state that increased investment in IT has a positive impact on corporate performance. Of course, these studies did not simply emphasize investment in IT. They emphasized the importance of harmony with IT security investments [80] and alignment with corporate management strategies [14].

However, even after setting aside the ongoing IT debate since Robert Solow's (1987) IT Productivity Paradox [31], the issue remains relevant. Managers' choices regarding the proportion of their investment in the IT sector should be flexible. These decisions must account for corporate characteristics and the business environment.

Lee, Shin, and Lee (2022) also revealed in their study on the introduction of 4th industrial revolution technologies and corporate productivity that the outcomes vary among companies. They note that the results of introducing new technologies such as IT may appear with a time lag [19].

Additionally, Winarno, Tjahjadi and Irwanto (2021), as well as Park, Koo, Ham and Lee (2006), presented similar findings. They showed that financial returns on resources invested in IT informationization and other growth foundations require a certain amount of time. These results partially support the findings of the present study.

Fourth, information security management tools, such as ISMS, should be flexibly considered for adoption by companies with a future growth-oriented management structure. Specifically, in the moderation effect analysis of ISMS(P) and ISO/IEC certification status on sales revenue, the adoption of information security management tools had a notable impact. The strategic use of tools such as the ISMS significantly strengthened the negative effect of H7-4 (CISO+CIO dual-role operation). This also mitigates the negative effect of H7-5 (IT investment ratio), shifting it in a positive direction.

Notably, the moderating effect of mitigating the negative impact of the proportion of IT investment on the IT department was also confirmed. Based on these findings, two security management strategies are proposed.

 doi:10.20944/preprints202506.1578.v1

First, for small and medium-sized venture companies or technology-based firms, where R&D is a core management strategy, having a CISO + CIO dual role may be unavoidable. In such business environments, the timing of adopting information security management tools, such as an ISMS, should be flexibly applied based on the company's situation. For example, when small-scale, R&D-focused IT-based technology companies need to launch products or services quickly, strict adoption of tools such as an ISMS may not be suitable. In such cases, these tools may hinder competitiveness in fast-paced environments.

Research on the effects of the CISO's dual roles and the mutual effects between the CISO and the ISMS is an important area of interest in information security. Choi and Kim (2024) measured the correlation between the CISO's dual roles and the adoption of information security management tools, such as ISMS [30]. Additionally, Ciekanowski et al. (2024) explored how the CISO's role within the organization affects ISMS. They concluded that the CISO's strategic operations help prevent cybersecurity incidents and secure sustainable competitive advantages [28].

However, this analysis has limitations when proposing security management strategies tailored to corporate characteristics. It is also difficult to use these findings as a basis for determining the timing of ISMS implementation or identifying the appropriate target group of companies.

The next proposed security management strategy is that, in a corporate environment where continuous investment in IT is required, the adoption of information security management tools, such as ISMS, should be actively considered. Even if continuous investment in IT results in short-term negative effects on external growth and adds to ongoing management burdens, these challenges should not discourage action. It is still advisable for managers to consistently implement security management activities. This includes the adoption of ISMS and other information security management tools.

This is particularly effective for large companies with sufficient financial capacity to withstand short-term financial burden. This is supported by the results of the multiple regression analysis on the control variables, which showed that the larger the asset size, the more significant the positive impact on sales and operating profits.

In particular, Ilmudeen and Bao (2018) [15] empirically demonstrated the full mediating effect of IT resource management capabilities on corporate performance. This finding indirectly supports the results of this study. This reinforces the moderating effect of information security management tools such as ISMS, which incorporate managerial elements related to IT resources [15].

Finally, this reflects the research results showing that the proportion of investment in information security is unrelated to corporate performance. New investments in information security technology or security equipment are expected to be integrated into IT information systems as subordinate components. Due to the technical characteristics of IT, these investments are often patched together, resulting in concurrent investments. This is because they coexist within the IT Governance environment, making it difficult to discern their individual effectiveness [39, 80].

In a study by Shariffuddin and Mohamed (2020), which effectively explained the importance of IT Governance, it was confirmed that investments in IT and information security sectors cannot be separated [39]. Many previous studies have recognized the introduction of new security equipment or security technology as an element of innovation. They expect technological innovation to improve corporate performance [82].

However, it is now expected that this will be interpreted differently. Owing to changes in the IT environment, the IT sector cannot be separated from the information security sector.

6. Conclusions

This study verifies whether the security management activities implemented by managers in business practices affect the financial performance of companies, such as sales. In particular, this study confirms the moderating effect of information security management tools, such as the ISMS. It contributes academically by proposing practical policies and indirectly demonstrating that security management activities are elements of innovation.

 doi:10.20944/preprints202506.1578.v1

6.1. Practical Implications

First, it can raise managers' awareness of the increased business risks posed by security incidents such as IT hacking and information leaks. Heightened awareness is crucial for proactive risk management. In addition, it can provide a decision-making guide for strategic security management activities tailored to each company's characteristics and business environment.

Second, it provides a basis for reevaluating the role and strategic position of the CISO. This is important to realize the positive business benefits of security management activities. These benefits include improved operational efficiency and enhanced external trust.

Third, it can help raise awareness that the adoption and maintenance of information security management tools, such as ISMS, are necessary from a strategic management perspective.

6.2. Academic Implications

First, research on information security should not be limited to the prevention of cybersecurity incidents at the national or corporate levels. Managers should be accepted as essential elements of innovation, moving beyond the traditional concept of information security. Ultimately, this should be expanded to the concept of security management and incorporated into technology management.

Second, starting with this study, we can expect that research variables related to security management will continue to be developed, leading to the emergence of various follow-up studies.

6.3. Limitations of the Study and Future Research Directions

First, the latent variables influencing the relationship between corporate security management activities and financial performance are not clearly defined. This study mainly focused on an objective analysis. Consequently, there was insufficient consideration of the exploratory and qualitative components.

Second, while this study focused on a cross-sectional empirical analysis of its research objectives, measuring the longitudinal changes in each research variable could yield more robust results. In particular, observing IT investments over the long term could enrich the connections with prior studies.

Third, further subdivision of the sample companies is necessary to address the diverse research objectives more effectively. This allows for a more detailed and targeted analysis. In particular, securing additional research samples from small and medium-sized venture companies would be valuable. This would enable meaningful exploration of the security management activities of early stage firms with less than 300 billion KRW in revenue, which was not the focus of this study.

Supplementary Materials

Author Contributions: Conceptualization, H. C. and K. C.; methodology, H. C.; validation, H. C. and K. C.; formal analysis, H. C.; writing, H. C.; writing review and editing, H. C. and K. C.; and supervision, K. C. All authors have read and agreed to the published version of the manuscript.

Funding: This study received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used to support the findings of this study are included in the article.

Acknowledgments

Conflicts of Interest: The authors declare no conflicts of interest.

 doi:10.20944/preprints202506.1578.v1

References

1. Wikipedia contributors. (2024, April 22). 2024 United States telecommunications hack. Wikipedia.
2. Newman, L. H. (2024, March 20). *The worst hacks of 2024 so far*. *WIRED*.
3. Global Cybersecurity Outlook 2024. World Economic Forum.
4. Mmango, N., & Gundu, T. (2024, July). Cybersecurity as a competitive advantage for entrepreneurs. In Annual Conference of South African Institute of Computer Scientists and Information Technologists (pp. 374-387). Cham: Springer Nature Switzerland.
5. Seo Seung-woo. (2015). Security Economics: An Information Security Investment Guide for CEOs. Seoul: Seoul National University Press.
6. Hameed, M. A., & Arachchilage, N. A. G. (2019). On the impact of perceived vulnerability in the adoption of information systems security innovations.
7. Onibere, M., Ahmad, A., & Maynard, S. B. (2021). Dynamic information security management capability: Strategising for organisational performance.
8. Marhad, S. S., Abd Goni, S. Z., & Sani, M. K. J. A. (2024). Implementation of Information Security Management Systems for Data Protection in Organizations: A systematic literature review. Environment-Behaviour Proceedings Journal, 9(SI18), 197-203.
9. Bokhari, S. A. A., & Manzoor, S. (2022). Impact of information security management system on firm financial performance: perspective of corporate reputation and branding. American Journal of Industrial and Business Management, 12(5), 934-954.
10. Son, Tae-hyun. (2015). The Impact of Corporate Information Security Activities on Information Security and Information Management Performance.
11. Byun, Jae-hak. (2019). A Study on the Impact of Personal Information Protection Regulatory Compliance on the Competitiveness of IT Companies Based on Regulatory Perception.
12. Jung Seung-il. (2007). The Impact of Government Regulation on Corporate Technological Innovation Behavior. Science and Technology Policy Institute, Policy Research 2007-13.
13. Kim Kyung-hee. (2024). A Study on the Comparison of Effective Organizational Leadership According to Organizational Type: Focusing on Situational Theory. Social Welfare Management Research, 11(1), 1-22.
14. Mithas, S., & Rust, R. T. (2016). How information technology strategy and investments influence firm performance. Mis Quarterly, 40(1), 223-246.
15. Ilmudeen, A., & Bao, Y. (2018). Mediating role of managing information technology and its impact on firm performance: insight from China. Industrial Management & Data Systems, 118(4), 912-929.
16. Hayes, A. F. (2013). Introduction to mediation, moderation, and conditional process analysis: A regression-based approach. Guilford Press.
17. Jeon Seung-jae. (2020). Information Security Incidents That CISOs and DPOs Must Know: Hacking Judgments Analyzed by a Hacker-Turned-Lawyer. Seoul: Samil Info Mine.
18. Jang Sang-soo. (2020). Introduction to Information Security and Personal Information Protection Management Systems. Paju, Gyeonggi-do: Saengneung Publishing Co., Ltd.
19. Lee, S., Shin, G., & Lee, J. (2022). A Study on the Relationship between the Adoption of 4th Industrial Revolution Technologies and Productivity in Enterprises: Absolute Level and Relative Position. Journal of the Korean Innovation Society, 17(3), 251-279.
20. Yu, J. Y., & Lee, J. I. (2010). Information Security for the Diffusion of New IT Services. Korea Information Processing Society Review, 17(2), 10-17.
21. Humphreys, E. (2016). *Implementing the ISO/IEC 27001: 2013 ISMS Standard*. Artech house.
22. Oh Seok-hong, Son Tae-won, & Lee Chang-gil. (2024). Major Theories of Organization [6th ed.]. Paju, Gyeonggi-do: Beomunsa.
23. Julien Vehent. (2018). DevOps Security in Cloud Environments. (Translated by Hong Seong-min and Joo Seong-sik) Paju, Gyeonggi-do: Wikibooks.
24. Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *Mis Quarterly*, 1189-1210.

 doi:10.20944/preprints202506.1578.v1

25. Ahyun Kim, Yong Jin Kim. (2021). Digital Entrepreneurship and Corporate Performance. Business Administration Research, 50(1), 1-22.
26. Garavan, T., & O'Brien, F. (2024). Contingency theory. In *A guide to key theories for human resource management research* (pp. 67-72). Edward Elgar Publishing.
27. Lex Donaldson. (2003). The Theory of Organizational Fit. Seoul: Gyeongmunsa.
28. Ciekanowski, M., Żurawski, S., Ciekanowski, Z., Pauliuchuk, Y., & Czech, A. (2024). Chief information security officer: a vital component of organizational information security management.
29. Electronic Financial Supervision Regulations. (2011)
30. Choi, Donsu, and Kim, Taeseong. (2024). The Concurrent Role of the Chief Information Security Officer and Information Security Performance: Focusing on Information Security Disclosure Data. Korean Management Association, 28(1), 49-63.
31. Robert solow. (1987) "we'd better watch out", Newyork Times Book Review July 12, 1987p 36.
32. Sun, J., & Jiao, H. (2024). Emerging IT investments and firm performance: a perspective of the digital options. Chinese Management Studies, 18(2), 506-525.
33. Agustina, N., & Pramana, S. (2019). The impact of development and government expenditure for information and communication technology on Indonesian economic growth. *Asian Journal of Business Environment*, *9*(4), 5-13.
34. Gartner. (2024). 2024 Report. "Korea IT Spending Forecast."
35. Information and Communications Policy Research Institute. (2024).
36. Korea Institute of Science and Technology Planning and Evaluation. (2024). 2022 Research and Development Activity Survey.
37. Park, Sohyun, Koo, Bonjae, Ham, Yugun, & Lee, Gukhee. (2006). Information Technology Investment Costs and Effects: Analysis and Empirical Study of Domestic Companies. Information Systems Review, 8(3), 201-223.
38. Lee, Seokjun. (1999). A Study on the Management of Corporate Information Technology Expenditures. Journal of Management Information Systems, Korean Management Information Systems Association, 9(2).
39. Shariffuddin, N., & Mohamed, A. (2020, March). IT security and IT governance alignment: a review. In Proceedings of the 3rd International Conference on Networking, Information Systems & Security (pp. 1-8).
40. Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and CounterIntelligence*, *26*(3), 453-481.
41. Chawla, R. N., Goyal, P., & Saxena, D. K. (2023). The role of CIO in digital transformation: an exploratory study. Information Systems and e-Business Management, 21(4), 797-835.
42. Alghorbany, A., Che-Ahmad, A., & Abdulmalik, S. O. (2022). IT investment and corporate performance: Evidence from Malaysia. Cogent Business & Management, 9(1), 2055906.
43. Kosutic, D., & Pigni, F. (2022). Cybersecurity: investing for competitive outcomes. Journal of Business Strategy, 43(1), 28-36.
44. Broderick, J. S. (2006). ISMS, security standards and security regulations. *information security technical report*, *11*(1), 26-31.
45. Song, H., Lee, Y., & Kang, J. (2024). Analysis of major defects repeatedly identified in information security and personal information protection management system (ISMS-P) certification audits. Journal of the Korean Society of Industry and Technology, 25(4), 427–432.
46. Hong, S., & Park, J. (2020). Effective Operation of the Information Security and Personal Information Protection Management System (ISMS-P) Certification System. Journal of the Korean Society of Industry and Technology, 21(1), 634–640.
47. Korea Internet & Security Agency. (2024). Introduction to the Information Security and Personal Information Protection Management System Certification Information Security Rating System.
48. Ministry of Science and ICT. (2017). Notice on the Granting of Information Security Management Grades (No. 2017-7).

 doi:10.20944/preprints202506.1578.v1

49. Lee, S. W. (2021). The Impact of ISO 22301 and ISMS Certification on Business Continuity Performance: Focusing on Corporate Culture and Processes (Domestic Doctoral Dissertation). Soongsil University Graduate School, Seoul.
50. Jo, Joong-Ki. (2016). A Study on Changes in Corporate Value after Obtaining Information Security Management System (ISMS) Certification (Domestic Master's Thesis). Chungbuk National University Graduate School, Chungcheongbuk-do.
51. Bae Young-Sik. (2012). A Study on the Impact of Information Security Management System (ISMS) Certification on Organizational Performance. Journal of the Korean Society of Industry and Technology, 13(9), 4224-4233.
52. West, S. G., Finch, J. F., & Curran, P. J. (1995), Structural equation models with nonnormal variables: Problems and remedies. In R. H. Hoyle (Ed.), Structural equation modeling: Concepts, issues, and applications (pp. 56–75).
53. Go Byung-wook, & Kim Sung-tae. (2023). A Study on the Determinants of Small and Medium-sized Enterprise Growth: Focusing on Characteristics According to Growth Measurement Methods. Financial Planning Review, 16(3).
54. Science and Technology Policy Institute. (2023). A Study on the Innovation Characteristics of High-Growth Service Companies: Focusing on Innovation Activities and Innovation Outcomes.
55. Kim Jung-ho. (2023). A Study on the Current Status and Support Policies for Deep Tech Startups.
56. Lee, Kyu-jin. (2011). Operating Profit Sustainability and Managerial Accuracy in Predicting Operating Profit. Tax Accounting Research, 30, 1-17.
57. Moon, Seon-woong. (2024). A Comparative Study of Global R&D Firm Performance and R&D Investment Support Systems. Asia-Pacific Research, 31(1), 114-143.
58. Kim, Hyun-joo. (2023). A Review of Research Trends on the Financial Performance of Medical Institutions. Journal of the Korean Society of Nursing Administration, 29(1), 76-85.
59. Korea Credit Guarantee Fund. (2023). A Study on Predicting the Risk of Default in Equipment Construction Companies Using Corporate Financial Data.
60. Bhandari, P. (2023). Control Variables | What Are They & Why Do They Matter?.
61. Field, A. (2018). *Discovering statistics using IBM SPSS statistics* (5th ed.). SAGE Publications.
62. Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2013). *Applied multiple regression/correlation analysis for the behavioral sciences* (3rd ed.). Routledge.
63. Hayes, A. F. (2017). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach* (2nd ed.). Guilford publications.
64. Li, X., Zhao, L., Ren, J., Sun, Y., Tan, C. F., Yeo, Z., & Xiao, G. (2024, December). A Unified Framework to Classify Business Activities into International Standard Industrial Classification through Large Language Models for Circular Economy. In 2024 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM) (pp. 1422-1426). IEEE.
65. Korea Standard Industrial Classification. (2024).
66. Kakushadze, Z., & Yu, W. (2017). Open Source Fundamental Industry Classification. Data, 2(2), 20.
67. Shin Eun-hee. (2021). The Impact of Manufacturing Security Performance on Corporate Management Performance: Focusing on Production Departments.
68. Lee Heung-bae. (2022). A Study on the Relationship between Information System Operating Environment Factors and Performance in Small and Medium Manufacturing Companies.
69. Kim, S. J., & Kim, T. S. (2023). Analysis of Information Security Management System Certification and Organizational Characteristics Using Information Security Disclosure Data. Korean Society of Management Information, 25(4), 205-231.
70. National Intelligence Service (2024). National Information Security White Paper.
71. Kim, S. C., & Park, Y. S. (2022). Corporate Asset Composition and Performance: The Impact of Intangible Assets on Corporate Growth and Value. Accounting and Policy Research, 27(2), 59–84.
72. Lim Ji-young, & Han Joon. (2022). The Impact of ESG Activities on Management Performance: Focusing on Corporate Size and Disclosure Roles. Commercial Education Research, 36(6), 29–51.

 doi:10.20944/preprints202506.1578.v1

73. Rizka, N. R., & Ulfida, D. (2024). Asset growth and firm performance: The moderating role of asset utilization. *BAJ: Behavioral Accounting Journal*, 7(2), 118–135.
74. Rahima, A. Y., & Muid, D. (2023). The effect of financial performance and firm size on firm value: Case study of banking companies listed on the Indonesia Stock Exchange in 2018–2020. *Tax Accounting Applied Journal*, 2(1), 1–8.
75. Utami, S. W. (2023). The effect of financial performance and capital structure on company value with company size as a moderation variable. *Asian Journal of Economics, Business and Accounting*, 23(24), 112–123.
76. Fiana, F., & Endri, E. (2025). Corporate social responsibility and financial performance: The moderating role of firm size. *International Journal of Economics and Financial Issues*, 15(2), 244–251.
77. Han Jung-in and Lee Jin-sook. (2024). The influence of behavioral inhibition temperament on internalizing behavioral problems in infants: The moderating effect of maternal overprotection. Journal of Emotional and Behavioral Disorders, 40(3), 65–84.
78. Moon, Y. K. (2022). The influence of temperamental fear on emotional and anxiety problems in infants: Focusing on the moderating effect of attention regulation and the moderated moderating effect of attention regulation and parental co-parenting. Play Therapy Research, 26(1), 1–20.
79. Lee, C. S., Shin, E. M., & Kim, Y. S. (2024). Analysis of mediating effects, moderating effects, and moderated mediating effects using the case-centered PROCESS macro. Saeron.
80. Alharbi, A., & Gregg, D. (2022). The Impact of IT Investment and IT Security Intensity on Firm Performance. In Proceedings of (pp. 1-21).
81. Weishäupl, E., Yasasin, E., & Schryen, G. (2018). Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers & Security*, *77*, 807-823.
82. Park, J. H., Lee, J. S., & Bae, J. T. (2015). Technology introduction through licensing and innovation performance: Focusing on domestic manufacturing SMEs. SME Research, 37(3), 99-125.
83. Winarno, W. A., Tjahjadi, B., & Irwanto, A. (2021). Time lag effects of IT investment on firm performance: evidence form Indone sia. Jurnal Ekonomi Malaysia, 55(3), 89-101.